SoK: Post-Quantum PAKEs

Cryptographic Primitives, Design and Security

Nouri Alnahawi[1,3,4], David Haas[2], Erik Mauß[1,4] and Alexander Wiesmaier[1,3,4]

[1] University of Applied Sciences, Darmstadt, Germany
[2] Technical University, Darmstadt, Germany
[3] National Research Center for Applied Cybersecurity ATHENE, Darmstadt, Germany
[4] European University of Technology, European Union

Abstract. PAKE protocols are used to establish secure communication channels using a relatively short, often human memorable, password for authentication. The currently standardized PAKEs however rely on classical asymmetric (public key) cryptography. Thus, these classical PAKEs may no longer maintain their security, should the expected quantum threat become a reality. Unlike prominent security protocols such as TLS, IKEv2 and VPN, quantum-safe PAKEs did not receive much attention from the ongoing PQC integration efforts. Thus, there is a significant gap in awareness compared to PQC schemes that are subject to the official governmental and institutional standardization processes. In the work at hand, we provide a comprehensive overview of the existing PQC PAKEs focusing on their design rationales, authentication methods and used asymmetric key agreement primitives. We highlight their performance and properties as per their assumed security assurances and practical usage in applications. Moreover, we address PAKE designs that are still non-present in the PQC realm and discuss the possibility of their adaptation. Thus, we offer a detailed reference and derive future work for quantum-safe PAKEs.

Keywords: Systematization of Knowledge · Password Authenticated Key Exchange · Post-Quantum Cryptography · Public-Key Cryptography

1 Introduction

Ever since their emergence in the early nineties [BM92], Password Authenticated Key Exchange (PAKE) protocols became of great importance in the world of (applied) cryptography. According to [HvO22], PAKE applications can be be found in several scenarios such as credential recovery (e.g., ICloud and ProtonMail), device pairing (e.g., E-Passport, bluetooth and WLAN), and E2E secure communication (e.g., Thread and Blackberry Messager). As the name suggests, PAKEs are used to carry out a key exchange combined with password based authentication. In other words, they allow for establishing secure communication over an insecure channel, where a communication party can prove their identity using a (often human memorable) password or a PIN (Personal Identification Number). The original idea proposed by Bellovin and Merritt was to combine a symmetric encryption scheme with a public-key crypto-system [BM92]. Basically, one encrypts a crucial part of the asymmetric key agreement with a password (or a password-derived value), so that attackers can neither trace the outcome of the agreement back to a possible password, nor actively manipulate the asymmetric key agreement. According to Jablon [Jab96], this can be achieved through a low entropy password if the small password

E-mail: nouri.alnahawi@h-da.de (Nouri Alnahawi), david.haas1@stud.tu-darmstadt.de (David Haas), erik.mauss@stud.h-da.de (Erik Mauß), alexander.wiesmaier@h-da.de (Alexander Wiesmaier)

Date of this document: 2025-02-15.